UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

DAVID MIDDENDORF,
THOMAS WHITTLE,
DAVID BRITT,
CYNTHIA HOLDER, and
JEFFREY WADA,

Defendants.

18 Cr. 036 (JPO)

GOVERNMENT BRIEF IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS THE INDICTMENT

GEOFFREY S. BERMAN
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

Rebecca G. Mermelstein
Amanda K. Kramer
Jessica Greenwood
Assistant United States Attorneys

- Of Counsel –

TABLE OF CONTENTS

Table of Authorities

Cases

Statutes

Rules

Secondary Sources

I. PRELIMINARY STATEMENT

The defendants in this case stole and converted confidential PCAOB information in order to provide KPMG with an illicit advantage in congressionally mandated audit inspections. In seeking to dismiss the indictment, the defendants make two inherently self-contradictory arguments in an effort to convince the Court that their nefarious conduct falls into a unique legal lacuna unpunishable by any criminal statute. With respect to Count One, which charges a conspiracy to defraud the SEC in violation of 18 U.S.C. § 371, the defendants repeatedly stress that the PCAOB is a private nonprofit corporation and not a federal agency. With respect to the wire fraud counts alleging a defrauding of the PCAOB in violation of 18 U.S.C. § 1343, however, the defendants rapidly shift gears. For those charges, they argue instead that the PCAOB essentially functions as a government regulator and thus its confidential information is unprotected by the wire fraud statute. They accordingly argue that the PCAOB's information is uniquely unprotected by the criminal law and that such information can be stolen and used for illicit corporate advantage without fear of prosecution. The Government respectfully submits that this position is absurd on its face and must be rejected.

The defendants engaged in a multi-year scheme to wrongfully obtain valuable confidential information from inside the PCAOB and the Government will prove at trial that the defendants knew what they were doing was wrong at every step of the way. KPMG employees repeatedly encouraged insiders within the PCAOB to breach duties of confidentiality and loyalty by stealing internal company information about upcoming KPMG inspections. PCAOB insiders repeatedly breached those duties and passed the secret information to their confederates. That confidential information was central to the work of the PCAOB and had to be replaced at significant expense after the scheme came to light. The defendants created cover stories, used code, destroyed documents, and talked about buying "burner" phones – all in an effort to keep their conspiracy a

secret. They hoped to keep using this illicit corporate information to game the PCAOB's confidential inspection work and evade the SEC's efforts to ensure SOX enforcement and the proper auditing of company financials. The grand jury's indictment setting forth this conduct charges a straightforward scheme that falls within the heartland of Sections 371 and 1343.

The Government respectfully submits this memorandum of law in opposition to the defendants' motions to dismiss all counts of the indictment in this case. For the reasons that follow, the motions are without merit and should be denied.

II. FACTUAL & PROCEDURAL BACKGROUND

A. THE SEC & THE PCAOB

The United States Securities and Exchange Commission ("SEC") is an agency of the United States. The SEC is vested with the authority and responsibility to implement and enforce the nation's securities laws, including provisions of the Sarbanes-Oxley Act of 2002 ("SOX"). One way the SEC seeks to protect investors is by ensuring that the market receives accurate audited financial information with respect to publicly traded companies ("Issuers"). (Indictment ¶ 1.) Part of this legal responsibility includes the regulation of the accounting industry that performs such audits, including issuing regulations and bringing enforcement actions when appropriate. *See, e.g.*, 15 U.S.C. § 7202(a) (referencing the SEC's authority to issue regulations in furtherance of SOX); 15 U.S.C. § 7202(b)(1) (referencing the SEC's enforcement authority pursuant to SOX and related regulations).

The Public Company Accounting Oversight Board (the "PCAOB") is a nonprofit corporation created by SOX in the wake of the accounting scandals at Enron and Worldcom. The PCAOB is a self-regulatory organization modelled after analogous entities in the securities industry like the Financial Industry Regulatory Authority ("FINRA") that regulate and discipline their own members, subject to oversight by the SEC. (Indictment ¶¶ 4, 10.) Among other

responsibilities, the PCAOB inspects registered public accounting firms ("Auditors") in order to ensure that such firms comply with SOX, SEC and PCAOB rules, and professional standards. These inspections are mandated by SOX. *See* 15 U.S.C. § 7214. In these inspections, the PCAOB examines the work that Auditors have performed with respect to particular audits of Issuers. (Indictment ¶ 4.)

The PCAOB conducts inspections of Auditors pursuant to two programs: (i) the Global Network Firm ("GNF") program, which annually inspects the six largest United States accounting firms and their global affiliates; and (ii) a program for all other firms. The PCAOB maintains a dedicated team of inspectors for each of the firms in the GNF program. Each firm in the GNF program is required to provide information to the PCAOB on an annual basis, including about each audit of an Issuer conducted by the firm during the year. (Indictment ¶ 5.)

In the winter of each year, the PCAOB typically selects which of a GNF firm's audits will be closely reviewed as part of the annual inspection of that firm. Issuers whose audits are selected for review by the PCAOB are colloquially referred to as having themselves been selected for inspection. The PCAOB's selection is based on information provided by the GNF firms and months of internal work and analysis of a variety of factors, including how long it has been since an audit of a particular Issuer was inspected, the risk factors for the audit, and an interest in including some randomly selected engagements, among others. (Indictment ¶ 6.)

In order to track the various factors considered in making inspection decisions, as well as to track which audits have been selected for inspection, the PCAOB maintains a planning spreadsheet for each GNF firm (the "GNF Planning Spreadsheet"). The GNF Planning Spreadsheet is updated throughout the inspection planning process. (Indictment ¶ 7.) As set forth

in greater detail below, the PCAOB devotes substantial employee time and resources to the development of its lists of audits to be inspected.

The PCAOB treats as highly confidential its internal list of audits selected for inspection. To that end, the PCAOB will generally only inform an Auditor of an upcoming inspection after the audit work papers are finalized and cannot be edited or improved upon in anticipation of a PCAOB inspection. (Indictment ¶ 8.) PCAOB employees are trained regularly on the need to protect confidential PCAOB information like the audit inspection lists. (Indictment ¶¶ 12-14 (detailing PCAOB rules, trainings, and certifications relating to confidentiality of PCAOB information).)

As required by SOX, once the PCAOB inspection of an Auditor is complete, the PCAOB prepares a written inspection report ("Inspection Report") containing the findings of the PCAOB. An Inspection Report contains two sections. Part I of an Inspection Report summarizes the PCAOB's "comments" or findings with respect to individual audits for which deficiencies were identified. Barring appeal by an accounting firm, Part I of an Inspection Report becomes public 30 days after it is issued. Part II of an Inspection Report generally addresses systemic deficiencies in the accounting firm's overall quality control. Accounting firms are given a one-year period to remedy any deficiencies identified in Part II of an Inspection Report, which becomes public only if an accounting firm fails to remedy deficiencies to the PCAOB's satisfaction within that one-year period. (Indictment ¶ 9.)

The SEC relies on PCAOB Inspection Reports to carry out its regulatory, oversight, and enforcement functions. Indeed, SOX commands that "[a] written report of the findings of the Board for each inspection under this section . . . shall be . . . transmitted, in appropriate detail, to the Commission . . . accompanied by any letter or comments by the Board or the inspector, and

any letter of response from the registered public accounting firm." 15 U.S.C. § 7214(g)(1). SOX also provides that the PCAOB must identify in every inspection any acts or practices that may be in violation of SOX, SEC rules, or PCAOB rules and "report any such act, practice, or omission, if appropriate, to the Commission . . . ." 15 U.S.C. § 7214(c)(2). In turn, the SEC Office of the Chief Accountant ("OCA") reviews Inspection Reports to monitor Auditor quality. Negative inspection results carry various consequences for accounting firms. (Indictment ¶ 11.)

The OCA also reviews Inspection Reports to identify any comments revealing weaknesses with respect to the financial statements of particular Issuers and refers such matters to the SEC's Division of Corporation Finance and the SEC's Division of Enforcement. (Indictment ¶ 11.) SOX vests the SEC with responsibility to make and enforce rules and regulations as "necessary or appropriate in the public interest or for the protection of investors, and in furtherance of this Act." 15 U.S.C. § 7202. To that end, the SEC may take enforcement actions against parties who violate PCAOB rules. Section 7202(b)(1) provides that:

> A violation by any person of [SOX], any rule or regulation of the [SEC] issued under [SOX], or any rule of the [PCAOB] shall be treated for all purposes in the same manner as a violation of the Securities Exchange Act of 1934 (the "Act") . . . or the rules and regulations issued thereunder, consistent with the provisions of [SOX], and any such person shall be subject to the same penalties, and to the same extent, as for a violation of [the Exchange Act] or such rules or regulations.

Id. Using the information in Inspection Reports, the SEC can, and does, bring enforcement actions against Auditors for failing to adhere to SEC or PCAOB rules. *See, e.g.*, SEC Press Release No. 18-39, 2018 WL 1284286 (Mar. 13, 2018) (announcing SEC charges premised on conduct that violated "PCAOB standards requiring sufficient analysis and inquiry when using the work of another auditor"); SEC Press Release No. 12-223, 2012 WL 5449659 (Nov. 8, 2012) (announcing SEC charges based on auditing work that "did not conform to the standards" of the PCAOB, as

the auditor had falsely claimed in its opinion); SEC Press Release No. 09-88, 2009 WL 2629377 (Aug. 27, 2009) (announcing SEC charges and settlement involving the issuance of false audit reports that "failed to comply with [PCAOB] standards"); SEC Press Release No. 07-183, 2007 WL 2681103 (Sept. 13, 2007) (announcing SEC charges against 69 auditors premised on failure to register with the PCAOB and thus "evad[ing] the PCAOB's oversight authority").

B. KPMG

KPMG is a professional service company and accounting firm providing audit, tax, and advisory services headquartered in Manhattan, New York. KPMG serves as the auditor for more than 600 Issuers each year. Because KPMG is among the six largest auditors in the United States, KPMG is inspected as part of the PCAOB's GNF program. (Indictment ¶ 15.)

KPMG has faced significant criticism and scrutiny from the SEC because of its poor performance in PCAOB inspections. For example, in or about 2014, KPMG received approximately 28 comments in connection with the approximately 51 audits inspected by the PCAOB that year. This was approximately twice as many comments as the average number of comments received by KPMG's competitors. A significant percentage of the comments pertained to KPMG's banking clients and, in particular, to the treatment of allowance for loan and lease losses ("ALLL"). ALLL, which is a calculated reserve maintained by financial institutions for estimated credit risks within an institution's assets, is often a critical issue in the auditing of a financial institution as it implicates its safety and soundness and impacts earnings. (Indictment ¶ 16.)

As alleged in the Indictment, by February 2016 the SEC's Office of the Chief Accountant had grown frustrated with KPMG's poor inspection results and scheduled a meeting with senior

KMPG personnel. (Indictment ¶ 59.)[1] Defendant David Middendorf and other senior executives accompanied the Chief Executive Officer ("CEO") of KPMG to a meeting with OCA in which the Chief Accountant expressed concern about audit quality issues at KPMG. The firm acknowledged the concern, particularly with respect to the need to improve quality surrounding ALLL issues. (Indictment ¶ 60.) Thereafter, OCA had additional meetings with KPMG on audit quality, including with defendant David Britt. (*See* Indictment ¶ 61.)

Doing well in the PCAOB inspection process was very important to KPMG. In addition to problems with the SEC and the PCAOB, poor PCAOB inspection performance could negatively impact the firm's ability to attract and maintain audit clients. Indeed, KPMG routinely touted positive inspection results when it could in new client pitches. (Indictment ¶ 17.)

Accordingly, by at least in or about 2015, KPMG was engaged in efforts to improve its performance in PCAOB inspections. Among other steps, KPMG (i) recruited and hired former PCAOB personnel, including but not limited to defendant Cynthia Holder and cooperating witness Brian Sweet; (ii) retained a data analytics firm to assist in predicting which of KPMG's engagements would be inspected by the PCAOB; (iii) awarded bonuses to members of engagement teams that received no comments during an inspection; and (iv) implemented internal monitoring programs to oversee certain audit areas, including ALLL. (Indictment ¶ 18.)

KPMG's audit practice was supervised by the Vice Chair of Audit. Within the audit practice, the Department of Professional Practice ("DPP") was responsible for maintaining audit quality at KPMG. (Indictment ¶ 19.) Several subsidiary groups fell under DPP, including the

[1] At trial, the Government anticipates soliciting testimony that OCA began having concerns about audit quality at KPMG based on its poor performance in PCAOB inspections by at least as early as late 2014, following release of the PCAOB's 2013 Inspection Report for KPMG.

DPP Audit Group and the DPP Inspections Group. The DPP Audit Group was responsible for setting audit policy and training KPMG personnel on new and existing audit standards. The DPP Inspections Group was responsible for conducting internal quality control inspections and dealing with inspections conducted by the PCAOB. (Indictment ¶ 20.)

C. THE DEFENDANTS AND BRIAN SWEET

The defendants in this case consist of executives and employees of KPMG and the PCAOB who were separated from their respective employers after the illicit conduct alleged in the Indictment was discovered. Specifically: (1) defendant David Middendorf was at all relevant times KPMG's head of DPP and the National Managing Partner for the Audit Quality and Professional Practice Group; (2) defendant Thomas Whittle reported to Middendorf and was at all relevant times a KPMG Audit Partner in DPP and the National Partner-in-Charge for Quality Measurement; (3) defendant David Britt reported to KPMG's Chief Auditor (who in turn reported to Middendorf) and was at all relevant times an Audit Partner in DPP, Banking and Capital Markets; (4) defendant Cynthia Holder was employed at the PCAOB and assigned to KPMG inspections from approximately December 2011 through July 2015 before joining KPMG and reporting to Brian Sweet; and (5) defendant Jeffrey Wada was an Inspections Leader at the PCAOB from approximately 2014 through approximately March 2017. (Indictment ¶¶ 22-26.)

From approximately 2009 through approximately April 2015, Brian Sweet was employed at the PCAOB, where he rose to the level of Associate Director. For much of his time at the PCAOB, Sweet was assigned to the team tasked with inspecting KPMG. In or about May 2015, Sweet began working at KPMG as an Audit Partner in the DPP Inspections Group, where Sweet reported to Whittle. While employed at KPMG, much of Sweet's work focused on banking clients. Sweet was separated from KPMG in or about March 2017. (Indictment ¶ 21). Sweet has pled

guilty to conspiring to defraud the United States and to commit wire fraud and is cooperating with the Government.

D. OVERVIEW OF THE FRAUDULENT SCHEME

The defendants are charged for their participation in a scheme to defraud the SEC and the PCAOB by obtaining and disseminating confidential PCAOB information relating to which KPMG audits the PCAOB would be inspecting in 2015, 2016, and 2017, so that KPMG could illicitly use that confidential information to improve its performance in PCAOB inspections. (Indictment ¶ 27.) The nature of the defendants' scheme, including the methods and means through which they carried it out, is set forth in significant detail in the 53-page indictment, which includes 89 paragraphs of factual allegations.

In brief, KPMG faced a crisis in 2015. It was doing twice as badly as its peer firms on PCAOB inspections. (Indictment ¶ 16.) That meant more private sector scrutiny by the PCAOB. It meant more government scrutiny – and admonishments and warnings – from the SEC. (Indictment ¶¶ 59-61.) It meant KPMG was at a competitive disadvantage against its peer firms in client recruitment. (Indictment ¶ 17.) So KPMG made a number of internal changes in an effort to improve its PCAOB inspection results, the most important of which was recruiting former KPMG inspectors at the PCAOB to work for the firm, beginning with Brian Sweet. (Indictment ¶ 18.)

But it turned out that KPMG did not want Sweet just for his accounting skills. Upon Sweet's arrival at KPMG, Middendorf, Whittle, and Britt immediately began pumping Sweet for confidential inspection information that Sweet knew or had taken with him from his time at the PCAOB. (*See* Indictment ¶¶ 32-41.) Middendorf, Whittle, and Britt made clear to Sweet that his loyalty and value to KPMG depended on his ability to provide such inside information. (*See id.*) Thereafter, consistent with the defendants' encouragement and support, Sweet provided, and

continued to provide, confidential PCAOB information to KPMG throughout 2015, including information that Sweet obtained from PCAOB colleagues after leaving the PCAOB. (*See* Indictment ¶ 42.) At Middendorf's request, Sweet also disclosed to KPMG the list of internal risk factors used by the PCAOB in making its inspection selections so that KPMG could use that information to make additional inspection predictions using a data analytics firm. (*See* Indictment ¶¶ 43-46.)

In or about May 2015, after Middendorf, Whittle, and Britt began seeking confidential PCAOB information from Sweet, Sweet in turn solicited and obtained such information from Holder, who still worked at the PCAOB. (*See* Indictment ¶¶ 47-54.) At the time, Holder was actively seeking employment at KPMG, and Sweet was helping her by speaking to Whittle on Holder's behalf. *(See id.*) Holder, however, had falsely told the PCAOB Ethics Office that she was not seriously considering employment at KPMG so that she would not be precluded from continuing to work on KPMG inspection matters. (*See id.*) This allowed Holder continued access to confidential PCAOB information about KPMG, which she shared with Sweet. (*See id.*) Sweet, in turn, shared at least some of this information with Whittle, who communicated his approval to Sweet by asking him if he had opened his drawer and seen where his paycheck comes from. (*See id.*) Holder was subsequently hired by KPMG and, like Sweet before her, copied confidential PCAOB information from her PCAOB computer before leaving to join KPMG, a fact that she made known to Sweet. (*See id.* ¶ 55-57.)

Following her transition from the PCAOB to KPMG, Holder remained in frequent contact with another PCAOB colleague, defendant Wada. That contact proved useful, as from at least in or about August 2015 through at least in or about March 2016, and again in or about January and February 2017, Wada repeatedly disclosed confidential PCAOB information to Holder. Holder in

turn disclosed the information to Sweet, who told Middendorf, Whittle, Britt, and others at KPMG. Those illicit tips included some of the most important confidential information in the PCAOB's possession, including its 2016 audit inspection list, and its preliminary and final audit inspection selections for 2017. (*See, e.g.*, Indictment ¶¶ 58, 63-66, 73-78, 80-83.) During the time that Wada made these repeated disclosures to Holder in violation of his ongoing confidentiality obligations as a PCAOB employee, Wada made annual certifications as to his compliance with those confidentiality rules, sought promotion at the PCAOB while expressing frustration at his failure to obtain it, began actively seeking employment at KPMG, and accessed KPMG-related files at the PCAOB despite not being assigned to work on KPMG inspections. (*See, e.g.*, Indictment ¶¶ 14, 23, 58, 62-65, 73-81.)

This confidential information illicitly obtained from the PCAOB was highly valuable to KPMG, and the conspirators set about putting it to work for the firm. For example, in or about March 2016, Middendorf, Whittle, Britt, and Sweet initiated stealth re-reviews of all engagements that appeared on a list of PCAOB inspection targets that Sweet made clear to his confederates had come from a former PCAOB colleague. (Indictment ¶¶ 66-71.) Middendorf emphasized that the top priority was protecting KPMG's internal monitoring programs (such as KPMG's ALLL monitoring program), because having a failed inspection for an audit subject to a monitoring program would demonstrate that the programs were not working and would represent a systemic failure at the firm. (Indictment ¶ 67.) As a result of the stealth re-reviews, KPMG identified audit issues that had not previously been detected and made certain modifications to their workpapers that were not disclosed to the PCAOB or the SEC despite having been made after the time when changes were allowable. (*See* Indictment ¶ 72.)

At every step of the scheme, the acts and statements of the defendants revealed that they knew what they were doing was wrong. For example, both Middendorf and Whittle emphasized the need to keep the true nature of the reviews and the fact that they had the confidential inspection lists a secret. (Indictment ¶ 67.) Britt told a KPMG partner that his audit was going to be inspected by the PCAOB, said he could not tell him how he knew, and told him to "keep his mouth shut." (Indictment ¶ 68). Wada referred to the list of inspections as the "grocery list" in communications with Holder. (Indictment ¶ 80). And in response to an investigation initiated by the general counsel at KPMG, Sweet and Holder destroyed relevant documents, discussed using "burner" telephones to disguise their ongoing communications, and hatched outlandish plans to claim that Holder had received confidential PCAOB inspection information anonymously in the mail. (*See* Indictment ¶¶ 85-89.) Following discovery of the scheme, each of the defendants was separated from their respective employers. (*See* Indictment ¶¶ 21-26.)

E. THE GUILTY PLEA AND THE INDICTMENT

On January 5, 2018, Brian Sweet pled guilty pursuant to a cooperation agreement to a two-count Information, charging him with: (1) conspiring to defraud the SEC, an agency of the United States (Count One); and (2) conspiring to commit wire fraud against the PCAOB (Count Two).

On January 17, 2018, a grand jury in this District returned a five-count indictment against the defendants. Specifically, all five defendants were charged with: (1) conspiring to defraud the SEC, an agency of the United States (Count One); (2) conspiring to commit wire fraud against the PCAOB (Count Two); and (3) substantive wire fraud against the PCAOB in 2016 and 2017 (Counts Four and Five, respectively). Defendants Middendorf, Whittle, and Britt were also charged with a 2015 substantive wire fraud against the PCAOB (Count Three).

F. THE MOTIONS TO DISMISS

On April 13, 2018, the defendants filed joint and separate motions to dismiss the Indictment, as follows: (1) a motion to dismiss in which all defendants have joined (the "Joint MTD," Dkt. 57); (2) a supplemental brief by defendants Britt and Whittle (the "Britt & Whittle MTD," Dkt. 58); (3) a supplemental brief by defendant Middendorf (the "Middendorf MTD," Dkt. 59); (4) a motion by defendant Holder (the "Holder MTD," Dkt. 54); and (5) a motion by defendant Wada (the "Wada MTD," Dkt. 60) (collectively the "Motions to Dismiss").

III. ARGUMENT

The Motions to Dismiss raise a litany of challenges to the Indictment, which range from attacks on the sufficiency of the Government's pleadings and trial evidence to legal arguments about the meaning of "property" and the constitutionality of the Government's fraud theories. For the reasons detailed below, these attacks are without merit and the Motions to Dismiss should be denied.

A. APPLICABLE LAW RELATING TO MOTIONS TO DISMISS

On a pretrial motion to dismiss pursuant to Fed. R. Crim. P. 12(b), the allegations of the indictment must be taken as true. *See Boyce Motor Lines, Inc. v. United States*, 342 U.S. 337, 343 n.16 (1952); *United States v. Goldberg*, 756 F.2d 949, 950 (2d Cir. 1985). The law is well settled that "[a]n indictment returned by a legally constituted and unbiased grand jury . . . if valid on its face, is enough to call for trial of the charges on the merits." *Costello v. United States*, 350 U.S. 359, 365 (1956).

"Pursuant to Federal Rule of Criminal Procedure 7, 'the indictment or information must be a plain, concise, and definite written statement of the essential facts constituting the offense charged.'" *United States v. Vilar*, 729 F.3d 62, 80 (2d Cir. 2013) (quoting Rule 7(c) (alterations omitted)). To satisfy this rule, "an indictment need do little more than to track the language of the

statute charged and state the time and place (in approximate terms) of the alleged crime." *United States v. Yannotti*, 541 F.3d 112, 127 (2d Cir. 2008) (internal quotation marks omitted). Only in "very rare cases," such as those involving a refusal to answer questions before Congress, must an indictment specify "how a particular element of a criminal charge will be met." *United States v. Stringer*, 730 F.3d 120, 125-26 (2d Cir. 2013) (discussing the special case of *Russell v. United States*, 369 U.S. 749 (1962)). Otherwise, "[a]n indictment is sufficient if it 'first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense.'" *Stringer*, 730 F.3d at 124 (quoting *Hamling v. United States*, 418 U.S. 87, 117 (1974)); *see also United States v. Yannotti*, 541 F.3d at 127.

Even in cases involving very bare-bones charges, courts will not dismiss the indictment absent a showing of prejudice. *Stringer*, 730 F.3d at 124. Where a defendant has been given sufficient notice of the charges against him by means of, for example, a criminal complaint or discovery, prejudice will not have been shown, and the indictment should stand. *See, e.g.*, *id.* at 124-25; *Yannotti*, 541 F.3d at 127. Moreover, it is well settled that a facially valid indictment is not subject to challenge based on the quality or quantity of evidence. *See United States v. Williams*, 504 U.S. 36, 54 (1992). A defendant's arguments about the sufficiency of the evidence should be raised at trial and not in a motion to dismiss. *United States v. Trochelmann*, No. 98 Cr. 1276 (JFK), 1999 WL 294992, at *2 (S.D.N.Y. May 11, 1999).

In sum, these cases stand for the "well established principle" that "there is no summary judgment in criminal cases." *United States v. Elie*, No. S3 10 Cr. 0336 (LAK), 2012 WL 383403, at *1 (S.D.N.Y. Feb. 7, 2012).

B. COUNT ONE PROPERLY ALLEGES A CONSPIRACY TO DEFRAUD THE UNITED STATES

The defendants claim that Count One fails to allege a conspiracy to defraud the United States. Specifically, the defendants jointly argue that the Indictment fails to allege that the conspiracy "targeted" the SEC, or that there was an agreement to use deceitful or dishonest means to defraud the SEC. (Joint MTD Parts I.B-C.) These attacks on Count One are baseless.

The defraud clause of Title 18, United States Code, Section 371 makes it an offense for "two or more persons [to] conspire . . . to defraud the United States, or any agency thereof in any manner or for any purpose," if "one or more of such persons do any act to effect the object of the conspiracy." 18 U.S.C. § 371. "It is well established that the term 'defraud' as used in § 371 not only reaches schemes which deprive the government of money or property, but also is designed to protect the integrity of the United States and its agencies." *United States v. Nersesian*, 824 F.2d 1294, 1313 (2d Cir. 1987) (citing *United States v. Johnson*, 383 U.S. 169 (1966)).

As required by Fed. R. Crim. P. 7(c), Count One of the Indictment tracks the statutory language of the defraud clause, states the approximate time and place of the crime, and thereby provides adequate notice to the defendants of the charges against them. *See United States v. Stavroulakis*, 952 F.2d 686, 693 (2d Cir. 1992). Specifically, Count One alleges that "[f]rom at least in or about April 2015, up to and including at least in or about February 2017, in the Southern District of New York and elsewhere, [the defendants], and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to defraud the United States and an agency thereof, to wit, the SEC, in violation of Title 18, United States Code, Section 371." (Indictment ¶ 90.) The Indictment further alleges that "[i]t was a part and object of the conspiracy that [the defendants], and others known and unknown, willfully and knowingly, using deceit, craft, trickery and dishonest means, would and did defraud the United

States and an agency thereof, to wit, the SEC . . . ," and sets forth various overt acts committed by the defendants in furtherance of the charged conspiracy. (Indictment ¶¶ 91-92.) These allegations, standing alone, satisfy Rule 7(c)'s pleading requirements. Although nothing more is required to defeat the defendants' motions with respect to Count One, the Indictment also includes 89 paragraphs of detail about the nature of the scheme in which the defendants participated.

In their attacks on Count One, the defendants do not seriously contend that the Government has failed to track the statutory language of Section 371 or provide details on the alleged scheme to defraud. Rather, they move for summary judgment. They first argue that the Indictment does not sufficiently allege that the scheme to defraud was "targeted" at the SEC. Similarly, defendant Wada argues that the Indictment fails to allege that he "engaged in . . . deceptive or deceitful action directed at the SEC." As noted above, the Indictment does both these things. (*See* Indictment ¶ 90 (defendants "agreed together and with each other *to defraud the United States and an agency thereof, to wit, the SEC*") (emphasis added); Indictment ¶¶ 91-92 (defendants "*using deceit, craft, trickery and dishonest means*, would and did defraud the United States and an agency thereof, to wit, the SEC) (emphasis added).) Any attack on the sufficiency of those allegations is improper at the motion to dismiss stage and must be reserved for trial.

To be clear, the fact that the Indictment also alleges additional motivations for the crime does not change that one purpose of the defendants' scheme was to defraud the SEC. In *United States v. Gurary*, the Second Circuit squarely held that the "intent to defraud the United States may be incidental to another primary motivation or purpose." 860 F.2d 521, 525 (2d. Cir. 1988) (citing *United States v. Southland Corp*., 760 F.2d 1366, 1373 (2d Cir. 1985)). In *Gurary*, an IRS-related case, the Second Circuit upheld the defraud clause convictions, noting: "Impeding the IRS, though not defendants' primary purpose, was part and parcel of the scheme. At a minimum, defendants

knew the fictitious invoices would be recorded in corporate books and records, records on which corporate tax returns are based." *Gurary*, 860 F.2d at 525.

The defendants next attempt to heighten the pleading requirements for a Section 371 violation. "The elements of a conspiracy to defraud the United States (also known as a 'defraud clause conspiracy') are: (1) that [the] defendant entered into an agreement (2) to obstruct a lawful function of the government (3) by deceitful or dishonest means and (4) at least one overt act in furtherance of the conspiracy." *United States v. Shellef*, 507 F.3d 82, 104 (2d Cir. 2007) (internal brackets and citations omitted). Not content with this black-letter law, the defendants argue that the Government must also allege and prove "either an affirmative misrepresentation to the government or the breach of a duty owed to the government." (*See* Joint MTD Part I.C.)

This theory finds no support in the law of the Second Circuit. In fact, the opposite is true. The Second Circuit has repeatedly rejected the defendants' argument that in order to prove a violation of the defraud clause the Government must show that the defendant owed a direct duty of disclosure to the relevant government agency. In *United States v. Nersesian*, 824 F.2d 1294 (2d Cir. 1987), for example, the defendants were convicted of a defraud clause conspiracy to interfere with the Internal Revenue Service's ("IRS") lawful function of monitoring financial transactions by agreeing to structure bank transactions such that no individual transaction was for more than $10,000 and thus avoiding the bank filing a Currency Transaction Report ("CTR"). *Nersesian*, 824 F.2d at 1309-16. On appeal, the defendants argued that the conviction should be overturned because they owed no direct duty to the IRS and had no direct contact with the IRS. The Second Circuit rejected these arguments, holding:

> Thus, the fact that Maktabi, as an individual bank customer, had no duty to report transactions over $10,000 is not the operative issue as to whether he agreed to unlawfully defraud the United States by impairing and obstructing its lawful governmental functions of

> collecting data and reports of currency transactions in excess of $10,000. The IRS has an interest in receiving CTRs from financial institutions when customers arrange transactions in excess of $10,000. In order for this lawful governmental function to operate, it is imperative that reports be submitted by financial institutions. If Maktabi and his associates agreed to interfere with and to obstruct this lawful function of the IRS, they could properly be charged with a violation of the "defraud prong" of § 371.

Id. at 1313.[2]

Similarly, in *United States v. Ballistrea*, 101 F.3d 827 (2d Cir. 1996), the Second Circuit addressed a defraud clause conviction premised on interfering with the regulatory functions of the United States Food and Drug Administration (the "FDA"). The defendants were multi-level marketers who pushed products they knew were not FDA approved to others for sale to end users. *Balistrea*, 101 F.3d at 830-31. They instructed their downstream distributors to take care in evading detection by the FDA. *Id*. In upholding their convictions, the court roundly rejected the defendants' arguments that the statute required "the making of misrepresentations to agency officials or the submitting of false information to the agency." *Id*. at 832. *See also United States v. Bilzerian*, 926 F.2d 1285, 1301-02 (2d Cir.1991) (upholding Section 371 conviction for defrauding the SEC by failing to make accurate Section 13(d) disclosures, explaining that "the

---

[2] *See also Shellef*, 507 F.3d at 104-06 (defendants properly convicted of defrauding the IRS for falsely telling purchasers of highly-regulated chemicals that the sales would not result in excise-tax obligation, because unwitting purchasers were more likely to mislead IRS about taxable status of sales); *Gurary*, 860 F.2d at 525 (defendants created and sold phony invoices to third party that used this information on its tax returns; mere fact that defendants knew that false information could have been used by third party on its tax returns sufficient to sustain Section 371 conviction for defrauding IRS, even if defendants did not intend to commit tax fraud by selling invoices to third party); *United States v. Zarrab*, 15 Cr. 867 (RMB), 2016 WL 6820737, at *3-5 (S.D.N.Y. Oct. 17, 2016) (denying motion to dismiss defraud charge alleging interfering with OFAC regulatory function by sending wires with false information through banks); *United States v. Buck*, No. 13 CR. 0282 (VM), 2017 WL 4174931, at *6 (S.D.N.Y. Aug. 28, 2017) ("The Indictment need not allege that Buck lied directly to a United States Treasury official or IRS agent in order to sufficiently allege a violation of Section 371.").

SEC is charged with administering and enforcing securities laws, and in order to perform its function must receive accurate and truthful disclosure").

Faced with this unbroken line of Second Circuit precedent,[3] the defendants turn to the Ninth Circuit. *See, e.g.*, *Murphy*, 809 F.2d 1427, 1431-42 (9th Cir. 1987) (holding that "where [relevant regulations] do not impose a duty to disclose information, failure to disclose is not conspiracy to defraud the government"); *United States v. Caldwell*, 989 F.2d 1056, 1059 (9th Cir. 1993) (confirming Section 371 requires deceitful or dishonest means and noting that "obstructing government functions in other ways—for example, by violence, robbery, or advocacy of illegal action, can't constitute defrauding"). While the defendants might prefer to try this case in the Ninth Circuit, the Second Circuit's views on Section 371 control. But in any event, the scheme charged in the Indictment quite clearly involves deceptive and dishonest means and not mere nondisclosure or the disclosure of solely truthful information. The Indictment charges the theft of highly confidential information from the PCAOB so that a cabal of insiders at KPMG could illicitly and secretly use that information to game a regulatory regime imposed by Congress and administered by the SEC. (*See, e.g.*, Indictment ¶¶ 32-54, 59-61, 66-72.) As the Indictment alleges, and as the defendants well knew, the SEC relies upon the data generated by PCAOB audits to execute its mandate under Sarbanes-Oxley. Through their deceptive conduct, the conspirators schemed to ensure that the PCAOB—which, as noted previously, has a statutory duty under SOX both to perform inspections and to report the results of those inspections to the SEC—would

[3] To be clear, the defraud clause continues also to be used outside of the Second Circuit to prosecute deceitful conduct that impairs, obstructs and defeats the lawful functions of government agencies. *See, e.g.*, *United States v. Internet Research Agency LLC, et al.*, 18 Cr. 32 (D.D.C.) (DLF) (case brought by the Special Counsel's Office, charging a Russian organization and affiliated persons and entities with, *inter alia*, conspiring to defraud the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State for the purpose of interfering with the U.S. political and electoral process, including the 2016 presidential election).

unwittingly provide the SEC with a false and misleading view as to the integrity of its inspections or the quality of KPMG audits. *See generally Bilzerian*, 926 F.2d at 1302 ("[T]he SEC is charged with administering and enforcing securities laws, and in order to perform its function must receive accurate and truthful disclosure."). Accordingly, the foregoing cases are inapplicable.[4]

Finally, the fact that SOX itself does not separately create a criminal offense for embezzling confidential PCAOB information and using that information to undermine the integrity of the PCAOB inspection process is of no moment. As the Second Circuit has repeatedly made clear, "the impairment or obstruction of a governmental function contemplated by section 371's ban on conspiracies to defraud need not involve the violation of a separate statute." *United States v. Rosengarten*, 857 F.2d 76, 78-79 (2d Cir. 1988) (citing *Haas v. Henkel*, 216 U.S. 462, 479-81 (1910)); *United States v. Brasco*, 516 F.2d 816, 817-18 (2d Cir. 1975); *United States v. Peltz*, 433 F.2d 48, 51 (2d Cir.1970); *Falter v. United States*, 23 F.2d 420, 423 (2d Cir. 1928). *See also Ballistrea*, 101 F.3d at 832 ("[S]o long as deceitful or dishonest means are employed to obstruct governmental functions, the impairment need not involve the violation of a separate statute."). Congress did not need to add such a provision to SOX to criminalize such conduct because such a provision already existed in the defraud clause and the mail and wire fraud statutes. Congress is

[4] The defendants' reliance on the Second Circuit's decision in *United States v. Coplan*, 703 F.3d 46 (2d Cir. 2012), is likewise misplaced. The Court of Appeals did not, as the defendants suggest, hold that Section 371 requires an affirmative misrepresentation to the government or an omission in breach of a legal duty. Instead, *Coplan* reversed the defendants' convictions for insufficient evidence. *Coplan*, 703 F.3d at 63-72 (holding that government's evidence of a criminal conspiracy at trial was "equally consistent with good faith in [the defendant's] role" in providing complex legal advice as a tax attorney). Indeed, at least one case in this District has expressly rejected a similar motion to dismiss based on *Coplan*. *See United States v. Buck*, No. 13 CR. 0282 (VM), 2017 WL 4174931, at *6 (S.D.N.Y. Aug. 28, 2017) (holding that "[t]he Indictment need not allege that Buck lied directly to a United States Treasury official or IRS agent in order to sufficiently allege a violation of Section 371" and noting that "*Coplan* invalidated the defendants' convictions, not the sufficiency of the indictment").

presumed to know the law when it legislates. *See generally Dir., OWCP v. Perini N. River Assocs.*, 459 U.S. 297, 319 (1983); *Cannon v. Univ. of Chicago*, 441 U.S. 677, 696-98 (1979).

In sum, the Indictment plainly alleges the necessary elements of a defraud clause charge and provides ample factual detail with respect to the scheme. Even the most cursory review of a long line of Second Circuit cases including, but not limited to, *Shellef*, *Nersesian*, *Ballistrea*, *Bilzerian*, and *Gurary*, all support the conclusion that the scheme at issue in this case falls within the heartland of conduct prohibited by the defraud clause. The defendants, through deceitful and illicit means, compromised the integrity of a statutorily imposed regulatory regime that the SEC is vested with the responsibility of overseeing and enforcing. As alleged in the Indictment and as supported by the contours of SOX itself, the receipt of accurate and trustworthy PCAOB Inspection Reports is an integral part of the SEC's lawful function. (*See* Indictment ¶ 11.) *See also* 15 U.S.C. § 7214(g)(1) (commanding that every PCAOB inspection report, along with PCAOB comments, be relayed to the SEC); 15 U.S.C. § 7214(c)(2) (commanding that "in each inspection" the PCAOB identify any acts or practices that may be in violation of SOX, SEC rules, or PCAOB rules and "report any such act, practice, or omission, if appropriate, to the Commission . . ."). Accordingly, Count One properly alleges a conspiracy to defraud the United States.

C. WADA'S CHALLENGES TO COUNT ONE ARE ALSO WITHOUT MERIT

Wada separately argues that the Indictment must have alleged that he "made . . . statements to the SEC in furtherance of the alleged conspiracy." (Wada MTD Part III.B.) As set forth above and established explicitly in cases such as *Ballistrea*, no such requirement exists. Indeed, even the primary Supreme Court case cited by the defendants for this proposition holds otherwise. *See Tanner v. United States*, 483 U.S. 107, 129 (1987) ("The Government observes, correctly, that under the common law a fraud may be established when the defendant *has made use of a third party* to reach the target of the fraud . . . . The Government also correctly observes that the broad

language of § 371, covering conspiracies to defraud 'in any manner for any purpose,' puts no limits based on the method used to defraud the United States.") (emphasis added). Wada also joins his co-defendants in premature factual attacks on the Government's trial proof of fraudulent intent and the use of deceptive means in participating in the scheme. As previously discussed, a motion to dismiss is not the proper occasion to challenge the sufficiency of the evidence. *See, e.g.*, *United States v. Martin*, 411 F. Supp. 2d 370, 373 (S.D.N.Y. 2006) (rejecting argument that indictment failed to allege "intended harm," and thus the fraudulent intent element of the offense, because "the sufficiency of the government's evidence of . . . fraudulent intent is not considered on a motion to dismiss the indictment").[5]

In any event, the Indictment in this case provides ample indicia of Wada's fraudulent intent and deceitful conduct. Wada repeatedly embezzled confidential PCAOB information by converting it to his own use and the use of others in breach of his duties to his employer. (*See, e.g.*, Indictment ¶¶ 14, 23, 58, 62-65, 73-81 (alleging that Wada made repeated disclosures of confidential PCAOB information to KPMG at times when he was also making annual certifications of compliance with PCAOB confidentiality rules).) Embezzlement is an act of deception. *See United States v. Yip*, 930 F.2d 142, 147 (2d Cir. 1991) (noting in mail fraud context that "false or fraudulent pretenses, representations, or promises" include "the act of embezzlement, which is the fraudulent appropriation to one's own use of the money or goods entrusted to one's care by another") (quotations omitted).

[5] *United States v. Finnerty*, 533 F.3d 143 (2d Cir. 2008), is not to the contrary. *Finnerty* is an appeal from a post-trial grant of a judgment of acquittal. A Rule 29 motion is the proper time to raise a sufficiency claim; a motion to dismiss is not. *Finnerty* itself recognized this. *See Finnerty*, 533 F.3d at 146 (noting an earlier denial of a motion to dismiss the indictment).

Furthermore, as the Government will argue at trial, Wada's covert passing of his "grocery list" of confidential PCAOB inspection information to KPMG reflects his intent to undermine the SOX inspection process and the regulatory regime overseen by the SEC. As an active PCAOB employee, Wada was intimately familiar with the inspection process and the overall SOX regulatory regime. He knew exactly why his friends and confederates at KPMG wanted that information, what they would do with it, and how that undermined the inspection process and the validity of the Inspection Reports transmitted to the SEC.

Finally, Wada's (and the other defendants') citation to the Supreme Court's recent ruling in *Marinello v. United States*, 138 S. Ct. 1101 (2018) is of no relevance to this case. *Marinello* dealt with an entirely different, tax-specific statute, 26 U.S.C. § 7212(a), the text, structure, and history of which differ substantially from the defraud clause of Section 371. The Supreme Court has upheld the language in Section 371 and its predecessor statute against challenges for over one hundred years. *See Haas v. Henkel*, 216 U.S. 462, 476-80 (1910) ("The statute is broad enough in its terms to include any conspiracy for the purpose of impairing, obstructing or defeating the lawful function of any department of Government."); *Hammerschmidt v. United States*, 265 U.S. 182, 188 (1924) ("To conspire to defraud the United States means primarily to cheat the Government out of property or money, but it also means to interfere with or obstruct one of its lawful governmental functions by deceit, craft or trickery, or at least by means that are dishonest."). Nothing in *Marinello* calls those decisions or Section 371 into question.

Again, Count One sufficiently states a violation of Section 371 and should not be dismissed.

D. COUNTS TWO THROUGH FIVE PROPERLY ALLEGE WIRE FRAUD AND WIRE FRAUD CONSPIRACY

The defendants also argue, without merit, that the wire fraud allegations in the Indictment must be dismissed. (*See, e.g.* Britt & Whittle MTD Parts I-II; Middendorf MTD Parts I-II; Holder MTD Parts I-IV; Wada MTD Part C.) As with many of their attacks on Count One, several of these arguments are nothing more than disagreements about what the evidence will show at trial. Given the allegations in the Indictment, which track the language of the relevant statutes and provide the defendants with ample notice of the nature of the charges against them, Counts Two through Five easily withstand the defendants' motions to dismiss.

The wire fraud statute proscribes the use of wire communications in interstate or foreign commerce "in furtherance of 'any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises.'" *Fountain v. United States*, 357 F.3d 250, 255 (2d Cir. 2004) (quoting 18 U.S.C. § 1343). The Second Circuit has summarized the "essential elements" of wire fraud as: "(1) a scheme to defraud, (2) money or property as the object of the scheme, and (3) use of the . . . wires to further the scheme." *Id*. at 255 (internal quotation marks and brackets omitted). With respect to aiding and abetting, 18 U.S.C. § 2 provides that "[w]hoever commits an offense against the United States or aids or abets or counsels, commands or induces, or procures its commission, is punishable as a principal." 18 U.S.C. § 2. "As at common law, a person is liable under § 2 for aiding and abetting a crime if (and only if) he (1) takes an affirmative act in furtherance of that offense, (2) with the intent of facilitating the offense's commission." *United States v. Konopski*, 685 F. App'x 63, 65 (2d Cir. 2017) (quoting *Rosemond v. United States*, 134 S. Ct. 1240, 1245 (2014) and citing *Hicks v. United States*, 150 U.S. 442, 449 (1893) for proposition that "accomplice liability attaches to conduct done 'with the intention of encouraging and abetting' the crime").

To charge a conspiracy to commit wire fraud under 18 U.S.C. § 1349, the Government must allege that "(1) a conspiracy existed, (2) the defendant knew of it, and (3) the defendant knowingly and voluntarily joined it." *United States v. Moran*, 778 F.3d 942, 960 (11th Cir. 2015); *United States v. Wrobel*, 12-CR-125W, 2017 WL 3097611, at *4 (W.D.N.Y. July 21, 2017).

Counts Two through Five of the Indictment easily satisfy the pleading requirements set forth above. To begin, the substantive wire fraud counts allege, as required, the approximate time periods of the charged frauds, that the defendants "willfully and knowingly . . . participated in a scheme to defraud," that the object of the scheme was to obtain "the PCAOB's property in the form of valuable confidential information,"[6] and that the defendants "transmitt[ed] . . . information by email" in furtherance of that scheme. (*See* Indictment ¶¶ 96-101.) Such allegations suffice to allege the elements of wire fraud, including fraudulent intent. *See Fountain*, 357 F.3d at 255. In any event, such fraudulent intent is readily inferable from the nature of the alleged scheme, *see, e.g.*, *United States v. Martin*, 411 F. Supp. 2d 370, 373 (S.D.N.Y. 2006) (inferring fraudulent intent with regard to wire fraud count from nature of purported scheme), which is described in detail above. *See supra* at 9-12. In addition to liability as principals, the factual allegations of the Indictment support holding defendants Middendorf, Whittle, Britt, and Holder liable for aiding, abetting, counseling, commanding, inducing or procuring the commission of wire fraud by current and former employees of the PCAOB. The Indictment alleges, for instance, that Middendorf, Whittle, and Britt encouraged Sweet first to disclose confidential PCAOB information and then to obtain additional confidential PCAOB information in violation of the duties of confidentiality of

[6] The defendants' argument that such information does not constitute "property" for purposes of the wire fraud statute is addressed separately below.

Holder, Wada, and other PCAOB colleagues. (*See, e.g.*, Indictment ¶¶ 32-58, 63-66, 73-78, 80-83.)

Likewise, Count Two sufficiently pleads a violation of Section 1349. Count Two alleges the approximate time of the conspiracy, that the defendants "willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud," and sets forth the object of that conspiracy. (*See* Indictment ¶¶ 94-95.) In light of the abundance of factual detail set forth in the Indictment, nothing more is required.

To the extent that the defendants' arguments challenge the quality and quantity of Government's anticipated evidence at trial, such challenges are not proper in a motion to dismiss. *See United States v. Corbin*, 729 F. Supp. 2d 607, 611 (S.D.N.Y. 2010) ("[F]act questions raised by an Indictment are the province of the jury.") (internal quotation marks omitted) (quoting *United States v. Pirro*, 96 F. Supp. 2d 279, 283 (S.D.N.Y. 1999)). (*See, e.g.*, Holder MTD Parts III and IV (arguing, based on facts outside the Indictment, that Holder's disclosure of confidential PCAOB information to her employer was justified, and further arguing that Holder's "use" of PCAOB confidential information as alleged in the Indictment was not sufficiently tied to the embezzled information to create wire fraud liability).)

The separate attack on Count Three raised by Middendorf, Whittle, and Britt is equally without merit. These defendants essentially argue that because Sweet had improperly taken PCAOB information before arriving at KPMG without these defendants asking him to do so, the wire fraud scheme in 2015 was complete before these defendants convinced Sweet to share the confidential information with them. (*See* Britt & Whittle MTD Part I; *see also generally* Middendorf MTD.) The defendants are wrong. With respect to wire fraud schemes based on the embezzlement of confidential information, the crime is complete not when an insider obtains the

relevant information but when he uses such information for personal gain or provides it to a third party.

For example, in *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), an IRS contract employee was charged with wire fraud for improperly accessing individual taxpayer files. The First Circuit reversed his conviction because he only accessed the information, rather than also disseminating or otherwise using it. *Czubinski*, 106 F.3d at 1075. The First Circuit reasoned: "Had there been sufficient proof that Czubinski intended either to create dossiers for the sake of advancing personal causes or to disseminate confidential information to third parties, then his actions in searching files could arguably be said to be a step in furtherance of a scheme to deprive the IRS of its property interest in confidential information." *Id*. This conception of wire fraud is well in line with the Supreme Court's seminal case on this issue, *United States v. Carpenter*, 484 U.S. 19 (1987), which related to the embezzlement of confidential information from the Wall Street Journal. In *Carpenter,* the Court noted that "it is sufficient that the Journal has been deprived of its right to exclusive use of the information, for exclusivity is an important aspect of confidential business information and most private property for that matter." 484 U.S. 19 at 26-27.

In this case, the PCAOB's right of exclusive use to its confidential information was violated when Sweet disclosed that information to third parties, not when he obtained it during his employment at the PCAOB. Even setting aside his illicit downloading of information when leaving the PCAOB, Sweet necessarily left the PCAOB with some amount of confidential PCAOB information in his mind that he took with him to his new job. That, of course, is not a crime. The crime is using that information, including disclosing that information to your new employer.

Accordingly, the crime alleged in Count Three was not perfected until Middendorf, Whittle, and Britt solicited and obtained from Sweet the valuable PCAOB information.

In any event, the Indictment alleges still more. Count Three describes successful efforts by Sweet to solicit and obtain further confidential PCAOB information from Holder in or about May 2015. (*See* Indictment ¶¶ 47-54.) Sweet shared at least some of the information he obtained from Holder with Whittle, who communicated his approval to Sweet. (*See id.*) All of this conduct is *after* Middendorf, Whittle, and Britt encouraged Sweet to disclose confidential PCAOB information at their meeting on May 4, 2015. (Indictment ¶ 32.) Based on the allegations in the Indictment, it can easily be inferred that Middendorf, Whittle, and Britt are at the very least liable as aiders and abetters of Sweet's efforts to obtain further confidential PCAOB information from Holder later that month. Accordingly, this challenge to Count Three also fails.

In short, because the Indictment sufficiently charges the defendants with wire frauds and wire fraud conspiracy, the defendants' challenges to the sufficiency of Counts Two through Five of the Indictment should be rejected.

E. THE INDICTMENT ALLEGES A PROPERTY INTEREST COGNIZABLE UNDER THE WIRE FRAUD STATUTE

When the arguments dispensed with above are set aside, the defendants' sole remaining wire fraud claim is that the PCAOB's confidential information relating to its inspections regime – one of its central corporate operations – is not "property" subject to the protections of the wire fraud statute. To make this argument, the defendants pivot mightily. In their arguments against the defraud clause charge, the defendants repeatedly stress that the PCAOB is not a government agency. In attacking the wire fraud counts, however, the defendants nationalize the PCAOB,

treating it as a government agency and its information as government property.[7] As set forth below, the defendants are wrong on both the facts and the law. The PCAOB is not a government agency but rather a private entity that creates, compiles, and maintains confidential information in the course of exercising its corporate functions. The information at issue – confidential information central to the core function of a nonprofit corporation – easily and uncontroversially falls within the ambit of property protected by the wire fraud statue.

1. Applicable Law

a. *Carpenter* and the Protection of Confidential Information

As referenced above, *United States v. Carpenter*, 484 U.S. 19 (1987), stands as the seminal Supreme Court case defining the scope of wire fraud prosecutions relating to the misappropriation of confidential information. In *Carpenter*, the Supreme Court affirmed the mail, wire, and securities fraud convictions of a reporter who agreed to provide two stockbrokers (who were also convicted) with securities-related information prior to its appearance in the reporter's daily column in the Wall Street Journal (the "Journal"), upon which information the brokers traded, with the understanding that the Journal's future coverage would affect stock prices. *See generally id.*[8] In summary, the Court endorsed the notion that the wire fraud statute criminalized the embezzlement

[7] In this vein, the defendants' citation to statutes protecting *government* information in their joint brief is telling. They argue that applying the wire fraud statute here would "swallow up a litany of federal statutes criminalizing the disclosure of specific types of regulatory information and nullify the judgments Congress has made about the relative seriousness, and corresponding penalties, associated with these different types of disclosures." (*See* Joint MTD at 39.) As the defendants would readily agree, however, the PCAOB is not a government agency and its information falls outside the ambit of all of the statutes they cite.

[8] The Court was evenly divided as to the sufficiency of the securities fraud conviction for reasons not relevant here. The mail and wire fraud charges were affirmed by a unanimous Court.

and personal use or disclosure of confidential business information from an entity that trusted the relevant insider with such information.[9]

The defendants in *Carpenter* argued that their conduct did not constitute a scheme to defraud the Journal as defined by the mail and wire fraud statutes and that they did not obtain any money or property from the Journal, as required by those statutes. *Id.* at 25. The Court rejected those arguments. *Id.* In doing so, the Court distinguished the *McNally* line of cases rejecting the intangible right of honest services as a property interest under the statutes, holding:

> [T]the object of the scheme was to take the Journal's confidential business information—the publication schedule and contents of the "Heard" column—and its intangible nature does not make it any less "property" protected by the mail and wire fraud statutes. *McNally* did not limit the scope of § 1341 to tangible as distinguished from intangible property rights.

Id. The Court went on to note that "[c]onfidential business information has long been recognized as property" and agreed with the proposition that "the Journal's interest in the confidentiality of the contents and timing of" its column is "a property right." *Id.* at 25-26 (citing *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1001-1004 (1984); *Dirks v. SEC*, 463 U.S. 646, 653, n.10 (1983); *Bd. of Trade of City of Chicago v. Christie Grain & Stock Co.*, 198 U.S. 236, 250-51 (1905)). Notably, the Court did not require the Journal to sustain a monetary loss; rather, it held, "it is sufficient that the Journal has been deprived of its right to exclusive use of the information, for exclusivity is an important aspect of confidential business information and most private property for that matter." *Id.* at 26-27. In doing so, the Court noted the importance of confidentiality to the Journal's business activity. *See id.* at 26.[10]

---

[9] The Second Circuit reaffirmed that fraud includes the act of embezzlement in *United States v. Yip*, 930 F.2d 142 (2d Cir. 1991).

[10] A number of cases have since reaffirmed the principle that confidential information constitutes property in the context of wire fraud. *See, e.g., United States v. Wang*, 898 F. Supp. 758, 760 (D.

While *Carpenter* used the phrase "confidential business information," the Second Circuit has subsequently noted that this language from *Carpenter* "merely *describes* the confidential information in that case; it does not require that *all* confidential information must be of the same nature to be considered property." *United States v. Grossman*, 843 F.2d 78, 86 (2d Cir. 1988) (affirming the mail fraud conviction of a law firm associate who misappropriated information and rejecting argument that information did not constitute "property" because it was not of commercial value to the firm).

b. *Cleveland* and the Exercise of Sovereign Regulatory Power

Approximately thirteen years after *Carpenter*, the Supreme Court issued its decision in *Cleveland v. United States*, 531 U.S. 2 (2000). In *Cleveland*, the Supreme Court reversed a conviction for mail fraud where the defendant lied on an application to a Louisiana state agency for a video poker license, holding that state and municipal licenses do not constitute the "property" of a state agency licensor for purposes of Section 1341. *See generally id.* In so doing, the Court held that the State's core interest with respect to the licenses was "regulatory" in nature and that the issuance of the licenses was simply an "exercise[] of state police powers." *Id.* at 20-21.

The Court rejected the argument that the State held a property interest based simply on its right to issue, renew, and revoke the licenses, as those powers merely reflected Louisiana's "sovereign power to regulate." *Id.* at 23. It also noted that the State was not a participant in the

Col. 1995) (holding that a copyrighted computer file is "intangible intellectual property"); *United States v. Martin*, 228 F.3d 1, 16-17 (1st Cir. 2000) (upholding *Carpenter* wire fraud charge based on defendant's embezzlement of confidential information from a veterinary products company); *United States v. Willis*, 737 F. Supp. 269, 276 (S.D.N.Y. 1990) (finding business information provided by patients to psychologist was property because the owner of the intangible, though valuable, confidential information "had a pecuniary interest in the non-disclosure of the information").

gaming industry, but was instead merely its regulator, rejecting comparisons to the holder of a patent or the like. *Id*. The Court found that the receipt of fees and revenue by the State pursuant to this licensing regime did not convert the licenses into property. *Id.* Accordingly, the Court observed that the State received the majority of such fees and revenue only after it had issued the licenses and that a processing fee at the time of application was insufficient to create a property interest in the license. *Id.* at 22. The defendant also paid the State all applicable fees and revenue flowing from the license, obviating any argument of economic harm. *Id.* Federalism concerns also colored the Court's reasoning. The Court therefore declined to "approve a sweeping expansion of federal criminal jurisdiction in the absence of a clear statement by Congress," which would be effected by "subject[ing] to federal mail fraud prosecution a wide range of conduct traditionally regulated by state and local authorities." *Id.* at 24.

2. Discussion

The defendants jointly move to dismiss Counts Two through Five on the grounds that the confidential information embezzled from the PCAOB in this case is a regulatory interest not protected as property under *Cleveland*'s interpretation of the wire fraud statute. (*See* Joint MTD Parts II.A-B.) The defendants' attempt to apply *Cleveland* to this case is misguided. First, unlike the state agency at issue in *Cleveland*, the PCAOB is not a government actor. It is a nonprofit corporation. The defendants have not cited, and the Government is not aware of, any instance in which *Cleveland* has been applied in the context of a private actor. Second, and more fundamentally, the nature of the property here is wholly different from the interest at issue in *Cleveland*. This case relates to the embezzlement of confidential information, which has long been recognized as falling within the ambit of property protected by the wire fraud statute, while *Cleveland* related to the exercise of a state agency's sovereign powers in the granting or

withholding of government licenses. The Court's holding in *Cleveland* is inapposite. Accordingly, the defendants' argument must be rejected.

a. The PCAOB is a private corporation to which *Cleveland*'s concerns about sovereignty and government power do not apply.

At the heart of the defendants' *Cleveland*-based attacks on the applicability of the wire fraud statute is the premise that the PCAOB – which the defendants are forced to acknowledge is a "private nonprofit corporation" with "nongovernment status" (*see* Joint MTD at 4 (internal quotation marks omitted)) – should be treated like a government agency under *Cleveland* because it exercises "regulatory interests" and "sovereign power" on behalf of the government. (*See, e.g.*, Joint MTD at 29-30 (describing the PCAOB's role and interest in confidential inspection information as "regulatory" and stemming "from Congress's sovereign regulatory power, which it delegated to the PCAOB").)

The defendants are correct that the PCAOB exercises authority created by Congress. The defendants immediately go too far, however, in characterizing that authority as one of "sovereignty." The PCAOB is not a sovereign and is not a part of the federal government, a state government, or a foreign government. It cannot exercise sovereign power.[11] Because the PCAOB is not a government regulator, *Cleveland*'s concerns about sovereignty and the exercise of government power are inapplicable. *See Cleveland*, 531 U.S. at 23. To accept the defendants' argument, the Court would be required to make a significant departure from *Cleveland* and its

[11] Congress could not have been more clear: "The Board shall not be an agency or establishment of the United States Government, and, except as otherwise provided in this Act, shall be subject to, and have all the powers conferred upon a nonprofit corporation by, the District of Columbia Nonprofit Corporation Act. No member or person employed by, or agent for, the Board shall be deemed to be an officer or employee of or agent for the Federal Government by reason of such service." 15 U.S.C. § 7211(b).

progeny, applying it for the first time to non-state actors. *See, e.g., United States v. Hedaithy*, 392 F.3d 580, 596-97 (3d Cir. 2004) (rejecting defendants' *Cleveland*-based argument that score reports issued by a private testing company did not constitute property under the wire fraud statute, holding that the reasoning of *Cleveland*, which "was based on the conclusion that the issuance of government licenses is an exercise of a state's police power to regulate," was "wholly inapplicable"). This threshold issue is fatal to the defendants' *Cleveland*-based challenge.

Accepting the defendants' premise that the PCAOB should be treated as a government regulator would also create the absurd result that the PCAOB – which enjoys none of the protections of actual government agencies, like the prohibition on the theft of government property under 18 U.S.C. § 641 – would likewise be deprived of the protections that private corporations enjoy under the wire fraud statute. Extending *Cleveland* for the first time into the private sector could exclude a wide swath of not-for-profit entities and their confidential information from the protections of the wire fraud statute,[12] including other self-regulatory organizations like FINRA and state and local bar associations. Neither the law nor policy supports such an outcome.

[12] Indeed, nonprofit corporations have long been recognized to have the same legal rights and remedies as for-profit corporations, including the protections of the wire fraud statute. *See, e.g., United States v. Detroit Med. Ctr.*, 833 F.3d 671, 674-75 (6th Cir. 2016) ("For centuries, courts have permitted charitable organizations to be treated as corporations . . . . So firm is the foundation on which this principle rests that Chief Justice Marshall's invocation of it in *Dartmouth College*—permitting a college to be treated as a corporation—might have been called cliché in 1819 . . . . By 1833, Justice Joseph Story was piling on when he wrote that charitable corporations may take the corporate form to the same degree as for-profit, commercial corporations . . . .") (internal citations omitted) (citing *Trs. of Dartmouth Coll. v. Woodward*, 17 U.S. 518, 636 (1819) (Marshall, C.J.) and 3 Joseph Story, *Commentaries on the Constitution* § 1386 (1833)). *See also, e.g., United States v. Oren*, 893 F.2d 1057, 1060-62 (9th Cir. 1990) (wire fraud on nonprofit organization); *United States v. King*, No. 98-CR-91A, 2000 WL 362026, at *7-12 (W.D.N.Y. Mar. 24, 2000) (wire fraud on not-for-profit charity).

b. Even if the PCAOB were inappropriately treated like a government agency under *Cleveland*, its confidential information would still be protected under the wire fraud statute.

Even if the PCAOB were treated as a government entity – which it certainly is not – the confidential information embezzled from the PCAOB, unlike the regulatory decision-making authority at issue in *Cleveland*, is in the heartland of information property interests protected by the wire fraud statute. In addition to cases such as *Martin* and *Wang*, which apply *Carpenter* to theft of information from businesses, *see supra* n. 10, other notable cases have applied *Carpenter* in the context of information held by a federal government agency. While these cases predate *Cleveland*, none found *Carpenter* inapplicable because the information at issue was confidential but not "business information." Indeed, neither the defendants nor the Government has identified a single case in which a court refused to apply wire fraud to a taking because the property stolen was "confidential information" but not "confidential *business* information."

For example, in *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991), a former Department of Defense employee was convicted of wire fraud for stealing secret documents from the Department and providing them to his new employer, Boeing (and certain other defense contractors). On appeal, the defendant challenged the applicability of Section 641, the statute criminalizing the theft of government property, but not the application of the wire fraud statute. Nevertheless, the Fourth Circuit, in upholding the conviction, cited *Carpenter* for the principle that this kind of information constitutes property under Section 1343. *Id*. at 310.

In *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), discussed briefly above, an IRS contract employee was charged with wire fraud for improperly accessing individual taxpayer files. The First Circuit reversed his conviction because he only accessed the information, rather than also disseminating or otherwise using it. *Czubinski*, 106 F.3d at 1075. In doing so, however, the Court of Appeals never suggested that *Carpenter* and its progeny were somehow inapplicable

to cases involving confidential government information because it was not "business information." The First Circuit agreed that "confidential information may constitute intangible 'property' and that its unauthorized dissemination or other use may deprive the owner of its property rights." *Id.* at 1074 (citing *Carpenter*, 484 U.S. at 26). The Court recognized that "[w]here such deprivation is effected through dishonest or deceitful means, a 'scheme to defraud,' within the meaning of the wire fraud statute, is shown." *Id.* (citing *Carpenter*, 484 U.S. at 27). The Court concluded: "Had there been sufficient proof that Czubinski intended either to create dossiers for the sake of advancing personal causes or to disseminate confidential information to third parties, then his actions in searching files could arguably be said to be a step in furtherance of a scheme to deprive the IRS of its property interest in confidential information." *Id*.

In light of these decisions, which continue to be cited as good law post-*Cleveland* (and given the stark absence of decisions reaching a different conclusion), there is simply no basis to conclude that the "confidential information" protected by *Carpenter* must be of commercial value or relating to commercial transactions. Indeed, the cases identified by the Government are to the contrary. For example, in *United States v. Kernell*, the court found that the contents of Sarah Palin's personal email account – including pictures – were property under the wire fraud statute. No. 3:08-CR-142, 2010 U.S. Dist. LEXIS 36477, at *8 (E.D. Tenn. Mar. 17, 2010). Citing *Czubinski*, the court rejected the defendant's claim that the information at issue need be economic or commercial in nature, focusing on the simple fact that Palin's property interest in the information was harmed when she lost exclusive control over its contents. *Id.* at *11-12. *See also Grossman*, 843 F.2d at 85-86 (affirming *Carpenter*-based conviction for theft of law firm information with no intrinsic commercial value).

Accordingly, for the reasons set forth above, the PCAOB information in this case qualifies as "confidential information" protected from misappropriation under *Carpenter*.

c. Although not required, the confidential information stolen has a significant financial value to the PCAOB and is not a mere regulatory interest.

Although *Carpenter* and its progeny make further analysis unnecessary, the information stolen in this case was of significant financial value to the PCAOB and not akin to the mere regulatory interest at issue in *Cleveland*. Accordingly, far from existing at the margins, the confidential information at issue here falls within heartland of "property" for the purposes of the wire fraud statute.

As a not-for-profit corporation, the PCAOB is in the business of conducting inspections of auditing companies. It routinely and regularly generates inspection lists in furtherance of that nonprofit mission. Indeed, the PCAOB could not conduct its core activities effectively without the confidentiality of its inspection selections. Accordingly, when the defendants in this case stole confidential inspection selections and related information from the PCAOB, they stole information that the PCAOB generates and uses in the exercise of its daily activities – not merely the PCAOB's final decision as to whether to issue a negative "comment" about a particular audit.

Importantly, the PCAOB's confidential selection information was of financial value, not just in the hands of the KPMG employees who wrongfully obtained it but also to the PCAOB. The PCAOB expends significant resources to create its inspection lists. As alleged in the Indictment, the PCAOB makes its inspection selections using information provided by audit firms and after "months of analysis of a variety of factors," which are tracked in an internal planning spreadsheet. (*See* Indictment ¶¶ 6-7.) The Government anticipates that its evidence at trial will include testimony from PCAOB employees about the time and expense involved in this process, which requires full-time work by numerous employees over weeks at a time each year. *Accord Bd. of*

Trade of City of Chicago v. Christie Grain & Stock Co., 198 U.S. 236, 250 (1905) (holding the collection and dissemination of commodity prices by the Chicago Board of Trade ("CBOT"), an entity incorporated by special charter of the state of Illinois, was entitled to protection and that the CBOT "has the right to keep the work which it has done, or paid for doing, to itself"). Furthermore, the Government expects that its trial evidence will show that, after the PCAOB discovered that its 2017 inspection selections had been improperly obtained by the defendants, the PCAOB was forced to re-create the KPMG inspection list for 2017 at significant expense so that the inspections would be confidential before announcement—a critical component of their utility. In addition to expending time and effort to create and re-create its inspection selections, the PCAOB also takes significant steps to maintain the confidentiality of that information, including through ethics trainings and regular certifications by PCAOB employees as to their compliance with PCAOB confidentiality rules. (*See, e.g.*, Indictment ¶ 14.)

These facts stand in stark contrast to the regulatory licenses at issue in *Cleveland*. There, the defendants deprived the state licensing authority only of an ability to make an informed regulatory decision about the issuance of licenses in the absence of fraudulent representations. As the Supreme Court put it, the state licensing authority lost only the "intangible rights of allocation, exclusion, and control [which] amount to no more and no less than Louisiana's sovereign power to regulate." *Cleveland*, 121 S. Ct. at 23. But nothing else was taken. The defendants did not scheme to embezzle the agency's files as in *Czubinski*, or its documents as in *Fowler*, or the confidential information in this case that allowed the PCAOB to conduct its nonprofit daily business. Furthermore, the state government in *Cleveland* suffered no economic harm as a result of being deceived in its regulation of licensing. The state simply issued a license that it otherwise might not have—essentially a costless act. Even more, as the Supreme Court repeatedly noted,

the state received all of the fees and tax revenue to which it was due notwithstanding having been deceived in the issuance of the license. *See id.* at 22. The state was in exactly the same place financially after the crime as before. Here, by contrast, the PCAOB spent significant sums creating its inspection lists and attempting to keep them confidential, in addition to sums necessary to generate a new list to perform its core corporate functions after the embezzlement of the 2017 inspection information.

For all of the reasons above, the confidential information misappropriated from the PCAOB in this case is cognizable as property under the wire fraud statute as interpreted by *Carpenter*. The defendants' arguments to the contrary should be rejected.

F. THE INDICTMENT IS NOT VOID FOR VAGUENESS

1. Applicable Law

The void-for-vagueness doctrine, rooted in the Due Process Clause of the Fifth Amendment, "requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *United States v. Morrison*, 686 F.3d 94, 103 (2d Cir. 2012) (quoting *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). The first prong requires a court to determine "whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal." *United States v. Roberts*, 363 F.3d 118, 123 (2d Cir. 2004) (quoting *United States v. Lanier*, 520 U.S. 259, 267 (1997)). "[A]lthough clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute, due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *Id.* (quoting *Lanier*, 520 U.S. at 266). Under the second, "more important," prong, *Kolender*, 461 U.S. at 358, the inquiry is "whether the statutory language is of such a standardless

sweep that it allows policemen, prosecutors, and juries to pursue their personal predilections." *Arriaga v. Mukasey*, 521 F.3d 219, 228 (2d Cir. 2008) (quoting *Smith v. Goguen*, 415 U.S. 566, 575 (1974) (internal quotation marks and alterations omitted)). "A statute that reaches 'a substantial amount of innocent conduct' confers an impermissible degree of discretion on law enforcement authorities to determine who is subject to the law." *Id.* (quoting *City of Chicago v. Morales*, 527 U.S. 41, 60-61 (1999)).

"Vagueness challenges to statutes not threatening First Amendment interests are examined in light of the facts of the case at hand; the statute is judged on an as-applied basis." *United States v. Coppola*, 671 F.3d 220, 235 (2d Cir. 2012) (quoting *Maynard v. Cartwright*, 486 U.S. 356, 361 (1988)). In such cases, regardless of whatever ambiguities may exist at the outer edges of the statute, a defendant cannot successfully raise its purported vagueness if his own alleged conduct is clearly prohibited. *United States v. Nadirashvili*, 655 F.3d 114, 122 (2d Cir. 2011). "[E]ven if there might be theoretical doubts" regarding whether a statute's contours could be clearly understood in every context, a "defendant's vagueness challenge fail[s] [if] his 'case presented no such problem.'" *Holder v. Humanitarian Law Project*, 561 U.S. 1, 22-23 (2010) (quoting *Scales v. United States*, 367 U.S. 203, 223 (1961) (alteration omitted)). Simply put, "one whose conduct is clearly proscribed" by a law may not challenge the law on the ground of vagueness. *United States v. Strauss*, 999 F.2d 692, 698 (2d Cir. 1993); *accord, e.g.*, *United States v. Amer*, 110 F.3d 873, 878-79 (2d Cir. 1997).

2. Discussion

a. The conspiracy to defraud the United States charge alleged in Count One is constitutional.

In their joint motion, the defendants argue that the Court should strike down the defraud clause of Section of 371 in its entirety as constitutionally vague or, in the alternative, should pare

down that provision to its constitutionally permissible core. (*See* Joint MTD Part I.D.) For the reasons set for the below, both requests should be rejected.

Because the defendants have identified no First Amendment concerns at play in this case, the sole question appears to be whether Section 371 is void for vagueness as applied to the charges against the defendants in Count One of the Indictment; the Court need not reach any facial challenge to that provision. *Coppola*, 671 F.3d at 235 (quoting *Maynard*, 486 U.S. at 361). This is wholly dispositive of the defendants' arguments. The defendants try gamely to suggest that "no person in the Defendants' position would have fairly understood that obtaining and using confidential information from a third party would also defraud a government agency, absent any false statement to or duty to disclose to that agency." (Joint MTD at 22.) But the defendants were highly-educated professionals employed at either KPMG or the PCAOB armed with training on the SEC's efforts at accounting oversight. They knew that the Inspection Reports were sent to the SEC. There can be no doubt that they understood that conspiring to steal and use the PCAOB's confidential inspection information to obtain an unfair advantage in the SOX inspection process and to mislead the SEC violates the law.

Perhaps recognizing the weakness of an as applied challenge, the defendants attempt to raise a facial challenge to the defraud clause of Section 371 as well as the "*Klein* conspiracy gloss" on that provision. (*See* Joint MTD Part I.D. at 21.) For the reasons stated above, the defendants cannot raise a facial claim. But in any event, Section 371 as applied and interpreted by the Supreme Court is facially valid.

Although the defendants attempt to undermine the precedential value of the so-called "*Klein* conspiracy gloss" by emphasizing its development in the Second Circuit's *Klein* decision, the *Klein* case simply quotes and applies the rule adopted by the Supreme Court in *Hammerschmidt*

v. United States, 265 U.S. 182 (1924). *See, e.g.*, *United States v. Klein*, 247 F.2d 908 (2d Cir. 1957) ("The statute, however, not only includes the cheating of the Government out of property or money, but "also means to interfere with or obstruct one of its lawful governmental functions by deceit, craft or trickery, or at least by means that are dishonest") (quoting *Hammerschmidt*, 265 U.S. at 188). That ruling, in turn, was long ago ratified by Congress when, in 1948, against the well-established backdrop of *Hammerschmidt* and its interpretation of the phrase "defraud the United States in any manner or for any purpose," Congress codified the current conspiracy statute employing that language and extending its application to "any agency" of the United States. *See* Act of June 24, 1948, ch. 645, 62 Stat. 701 (enacting 18 U.S.C. § 371). As the Supreme Court has repeatedly explained, "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." *Forest Grove Sch. Dist. v. T.A.*, 557 U.S. 230, 239-240 (2009) (quoting *Lorillard v. Pons*, 434 U.S. 575, 580 (1978)).

The defendants offer no serious argument that the Supreme Court's construction of the defraud clause, as incorporated by Congress – which encompasses conspiracies that "interfere with or obstruct . . . lawful government functions by deceit, craft, tricky, or . . . dishonest" means – is beyond the ability of "ordinary people [to] understand," *see Morrison*, 686 F.3d at 103 (quoting *Kolender*, 461 U.S at 357). The defendants likewise cite no authority in support of their novel proposition that the Supreme Court's own interpretation of a criminal statute could create constitutional vagueness concerns.

Instead, the defendants attempt to bolster their constitutional argument by citing a law review article opining as to the statute's vagueness, as well as a case that references the breadth of criminal conspiracies generally in the course of addressing a Section 371 challenge. *See, e.g.*,

Dennis v. United States, 384 U.S. 855, 859 (1966) (citing cases involving conspiracy to violate the White Slave Traffic Act and conspiracy to commit perjury in support of general proposition that "inherent in a criminal conspiracy charge [is the possibility] that its wide net may ensnare the innocent as well as the culpable"). The defendants also cite cases that, while acknowledging case law firmly establishing the breadth of Section 371, do so in the course of discussing why the application of the statute should not be further enlarged, *see United States v. Rosenblatt*, 554 F.2d 36, 40 (2d Cir. 1977) (noting need to protect against "attempts to broaden" the scope of conspiracy prosecutions), or in affirming the validity of Section 371 and the *Klein* doctrine as consistent with longstanding precedent, *see United States v. Coplan*, 703 F.3d 107 (2d Cir. 2012) ("Notwithstanding these infirmities in the history and deployment of the statute, it is now well established that § 371 is not confined to fraud as that term has been defined in the common law, but reaches any conspiracy for the purpose of impairing, obstructing or defeating the lawful function of any department of Government."). None of these authorities supports a facial challenge to Section 371.

The defendants' attempted reliance on *United States v. Skilling*, 561 U.S. 358 (2010) and *United States v. Marinello*, 138 S. Ct. 1101 (2018) is also misplaced. With respect to *Skilling*, the defendants purport to identify "similar infirmities" between Section 371 and the honest services fraud statute, and argue based on those similarities that Section 371 should be deemed constitutionally deficient. However, the defendants all but ignore the fact that the Court in *Skilling* declined to overturn the honest services fraud statute on vagueness grounds. *See Skilling*, 561 U.S. at 405-08. The defendants also fail to quote the operative language that was challenged in *Skilling* – "to deprive another of the intangible right to honest services," *see id.* at 404 – which has no relevance to whether a conspiracy "to defraud" the United States under Section 371 is

impermissibly vague. Finally, the concerns raised in *Skilling* about a congressional attempt to resurrect a set of circuit decisions that "were not models of clarity or consistency," *see id.* at 405, do not apply here, where Congress has adopted longstanding and clear statutory-interpretation decisions of the Supreme Court. In short, and unsurprisingly, *Skilling* is neither applicable nor instructive so far afield from the honest services context.

Turning to *Marinello*, the defendants argue that the Supreme Court's rejection of a "broad interpretation of [a] statute criminalizing obstruction of the due administration of the tax code" based in part on vagueness concerns supports their challenge to Section 371. Again, however, the Court in *Marinello* addressed statutory language simply not at issue in the text of the defraud clause, *see Marinello*, 138 S. Ct. at 1104, which by its terms applies to schemes to defraud the United States or its agencies. In addition, the alleged scheme to defraud relates to the SEC's oversight of particular PCAOB inspections of the leaked Issuers from 2015, 2016, and 2017 – such that *Marinello*'s concerns about punishing obstruction broadly without relation to a particular proceeding are not implicated here.

In addition to rejecting the defendants' facial challenge to Section 371 for the reasons set forth above, the Court should decline the defendants' invitation to limit Section 371 to a permissible "core." No limiting construction is required to "save" the defraud clause of Section 371, which has important inherent limitations that guide its use, including the longstanding requirement that the means used to carry out the conspiracy be deceptive or dishonest. *See Hammerschmidt v. United States*, 265 U.S. 182, 188 (1924) ("To conspire to defraud the United States means primarily to cheat the Government out of property or money, but it also means to interfere with or obstruct one of its lawful governmental functions by deceit, craft or trickery, or at least by means that are dishonest.").

The defense request is also strongly undermined by the holding in *Coplan*. Although the defendants are correct that the appellants in *Coplan* attempted to overturn the longstanding rule that money or property damage is not required to state a *Klein* conspiracy charge, the Court of Appeals in that case made clear that it was "bound to follow the dictates of Supreme Court precedents" – including "well established [authorities holding] that Section 371 . . . reaches any conspiracy for the purpose of impairing, obstructing, or defeating the lawful function of any department of Government" – and could not "[a]s an intermediate appellate court . . . break[] loose from the moorings of established judicial norms by 'paring' a statute" in a manner akin to *Skilling*. *See Coplan*, 703 F.3d at 61-62. The defendants offer no reason to suggest that this court is in a better position to disregard "established judicial norms" than the Second Circuit.

Undeterred, the defendants dispense entirely with this well-established precedent in their suggested "paring," including by rejecting the Supreme Court's clear and expansive holdings in *Haas* and *Hammerschmidt* in favor of three limited categories of conduct they believe to be properly criminalized by Section 371. Conveniently, these categories of conduct have been crafted by the defendants so as to exclude the allegations in the Indictment, and to incorporate requirements such as an affirmative duty of disclosure that – as described above – have been explicitly rejected by the Second Circuit.[13] *See supra* at 17-20.

[13] Despite having crafted these categories of conduct themselves, the defendants nevertheless argue in the alternative that their second category of Section 371 conduct is also unconstitutional. (*See* Joint MTD at 24 n.1.) In other words, even if the Court were to limit Section 371 precisely as requested by the defendants, the defendants would maintain that this pared-down statute still violates the Constitution.

b. The wire fraud and wire fraud conspiracy charges alleged in Counts Two through Five likewise pass constitutional muster.

The defendants also argue – in a single sentence, with no specific analysis or support – that Counts Two through Five of the Indictment are void for vagueness. (*See* Joint MTD Part II.D; Wada MTD Part C.) Although the defendants devote a separate section of their joint brief to raising this constitutional challenge, the defendants do so entirely in passing after two paragraphs of attacks on the Government's theory, which the defendants characterize as internally inconsistent and shifting. Such critiques are properly viewed as attacks on the Government's ability to prove its case at trial, which are inappropriate on a motion to dismiss. In any event, the defendants' constitutional challenge to the wire fraud counts is as baseless as it is brief. Counts Two through Five, which set forth a straightforward scheme predicated on the embezzlement of confidential information from a nonprofit corporation using the wires, provide the defendants with ample notice of the conduct with which they are charged. Further, ordinary individuals in the defendants' positions would reasonably understand that engaging in such conduct or conspiring to do so is criminal. As such, Counts Two through Five are not unconstitutionally vague.

G. NEITHER STATUTORY CONSTRUCTION NOR THE RULE OF LENITY COMPELS DISMISSAL OF COUNTS TWO THROUGH FIVE.

1. Applicable Law

Under principals of statutory construction and the rule of lenity, "ambiguous criminal laws [are] to be interpreted in favor of the defendants subjected to them." *United States v. Banki*, 685 F.3d 99, 109 (2d Cir. 2012). The rule of lenity is applicable in very limited circumstances and only where "after considering text, structure, history, and purpose, there remains a grievous ambiguity or uncertainty in the statute." *Barber v. Thomas*, 560 U.S. 474, 488 (2010) (internal quotation marks omitted). *See also United States v. Edelman*, 726 F.3d 305, 309-10 (2d Cir. 2013). Emphasizing its narrow application, the Second Circuit has cautioned that "the rule of lenity is not

a catch-all maxim that resolves all disputes in the defendant's favor—a sort of juristical 'tie goes to the runner."' *United States v. Gonzalez*, 407 F.3d 118, 124 (2d Cir. 2005). In the absence of unresolved, grievous ambiguity, the rule of lenity has no application.

2. Discussion

The defendants' argument that statutory construction and the rule of lenity compel dismissal should be swiftly rejected. (*See* Joint MTD Part II.C.) Because the PCAOB is not a government agency, the defendants' concerns that the Government's theory in this case would render "all confidential information held for regulatory purposes at every level of government—federal, state, and local . . . 'property' for purposes of the wire and mail fraud statues," or would update the "detailed array of penalties [imposed by Congress] for disclosures of different kinds of regulatory information held across the federal government" are utterly baseless. (Joint MTD at 37-40.) As in the context of 10b-5 securities fraud cases, courts have repeatedly affirmed that "[n]ovel or atypical methods [of fraud] should not provide immunity from the securities laws." *United States v. Russo*, 74 F.3d 1383, 1390 (2d Cir. 1996) (quoting *Superintendent of Ins. v. Bankers Life & Casualty Co.*, 404 U.S. 6, 10 n.7 (1971) (quoting *A. T. Brod & Co. v. Perlow*, 375 F.2d 393 (2d Cir. 1967)). The same holds true here. As such, the allegations in the indictment are consistent with the text of the wire fraud statute and the rule of lenity.

Finally, the defendants close their principal motion papers by suggesting that Congress "chose" to leave the protection of PCAOB's confidential information to civil and administrative enforcement over criminal prosecution. (*See* Joint MTD at 42.) This claim is preposterous. It is highly unlikely that Congress foresaw that one day several members of one of the biggest accounting firms in the world would conspire with PCAOB insiders in a brazen scheme to steal its most precious confidential inside information and use it to defeat the SEC's efforts to ensure effective and reliable accounting in the aftermath of some of the biggest financial scandals of the

modern era. But Congress does not need to foresee every novel scheme and enact new laws to strike each down because it has passed the mail and wire fraud statutes.[14] The wire fraud statute squarely forecloses a scheme to steal confidential information from a private corporation through acts of deception.

IV. CONCLUSION

For the reasons set forth above, the defendants' Motions to Dismiss the Indictment should be denied.

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By: /s/ *Jessica Greenwood*
Rebecca G. Mermelstein
Amanda K. Kramer
Jessica Greenwood
Assistant United States Attorneys
(212) 637-2360 / 2478 / 1090

[14] *See generally* Jed S. Rakoff, *The Federal Mail Fraud Statute (Part I),* Duquesne Law Review, vol. 18 num. 4 (1980) at 772 ("The mail fraud statute, together with its lineal descendent, the wire fraud statute, has been characterized as the 'first line of defense' against virtually every new area of fraud to develop in the United States in the past century. . . . In many of these and other areas, where legislatures have sometimes been slow to enact specific prohibitory legislation, the mail fraud statute has frequently represented the sole instrument of justice that could be wielded against the ever-innovative practitioners of deceit.").